NORTH DAKOTA

HOMELAND SECURITY

ANIT-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Nothing Significant to Report

Regional

(South Dakota; Nebraska; Iowa) **U.S. Army Corps of Engineers to assess damage of Gavins Point Dam spillway slabs.** The U.S. Army Corps of Engineers said it will conduct a damage assessment of the spillway slabs at Gavins Point Dam on the Missouri River in Nebraska and South Dakota, May 9. The chief of the Omaha District hydrologic engineering branch said releases from the dam will be halted for no more than 8 hours to dewater the uppermost portion of the spillway. A preliminary assessment of damages sustained after the 2011 flood indicated minor damage to many areas on the slab. The investigation will include the use of ground penetrating radar and other methods to develop and implement corrective measures by the spring of 2013. Stage reductions at Yankton, Sioux City, and Omaha were expected to last for about 12 hours, 24 hours, and 48 hours, respectively. Source: http://www.therepublic.com/view/story/a925b23aba324f50902bf5929ffd21c3/SD--Gavins-Point-Assessment/

National

Cyber security is weakest link in state preparedness, according to FEMA survey. Although States have made huge strides in emergency and natural disaster preparedness, they are still vulnerable to cyber disasters, according to the Federal Emergency Management Agency National Preparedness Report released May 4. The study said despite progress across core areas such as planning and operational coordination for natural disasters, and information sharing among intelligence agencies on terror activity, States indicated cybersecurity was their weakest core capability. Source: http://www.gsnmagazine.com/node/26273

International

Nothing Significant to Report

Banking and Finance Industry

IC3 2011 Internet Crime Report released. The Internet Crime Complaint Center (IC3) May 10 released its 2011 Internet Crime Report — an overview of the latest data and trends of online criminal activity. According to the report, 2011 marked the third year in a row the IC3 received more than 300,000 complaints. The 314,246 complaints represent a 3.4 percent increase over 2010. The reported dollar loss was $485.3 million. In 2011, IC3 received and processed, on average, more than 26,000 complaints per month. The most common complaints received in 2011 included FBI-related scams — schemes in which a criminal poses as the FBI to defraud victims — identity theft, and advance-fee fraud. The report also lists States with the top complaints and provides loss and complaint statistics organized by State. It describes

complaints by type, demographics, and State. Source: http://www.ic3.gov/media/2012/120511.aspx

Business continuity preparedness. Many organizations are struggling to manage data in hybrid physical, virtual, and cloud environments; many still use multiple tools, which are likely to be spread across multiple sites, with just over a third (36 percent) managing three or more different solutions to protect critical data, according to Homeland Security Newswire May 10. Despite 2011 experiencing record levels of environmental, economic, and political upheaval, the 2012 Acronis Disaster Recovery Index findings from the industrial sector revealed that only 53 percent of respondents were confident they could recover quickly in the event of a disaster. Nearly half (45 percent) of those surveyed cited lack of budget and IT resources as their key challenges in data recovery. One in 10 (11 percent) said they spend nothing on backup and disaster recovery, and a quarter stated they do not have sufficient support from senior business executives. In a highly competitive sector where tolerance for downtime is extremely low, only 45 percent said they would not suffer substantial downtime in the event of a serious incident or natural disaster. Source: http://www.homelandsecuritynewswire.com/srdisasters20120510-only-half-of-industrial-firms-confident-they-could-recover-quickly-from-disaster

Identity thieves could rake in $26 billion in tax refunds. Criminals who file fraudulent tax returns by stealing people's identities could rake in an estimated $26 billion over the next 5 years because the Internal Revenue Service (IRS) cannot keep up with the amount of the fraud, the U.S. Department of the Treasury Inspector General for Tax Administration (TIGTA) said May 8. "Our analysis found that, although the IRS detects and prevents a large number of fraudulent refunds based on false income documents, there is much fraud that it does not detect," the inspector general said in prepared testimony before a joint hearing of two House subcommittees. The TIGTA report is the first detailed analysis of the tax refund fraud problem, which could affect any taxpayer. His projection of $26 billion was larger than any other estimate of identity theft tax fraud. In 2011, according to TIGTA, the IRS reported that of the 2.2 million tax returns it found to be fraudulent, about 940,000 returns totaling $6.5 billion were related to identity theft. In the investigation, the inspector general said auditors found another 1.5 million undetected tax returns with more than $5.2 billion in fraud. As of April, the IRS reported it had stopped the issuance of $1.3 billion in potentially fraudulent tax returns. Source: http://www.cnn.com/2012/05/08/us/tax-refund-fraud/index.html?hpt=hp_t3

Tatanga malware platform used in fraud insurance scam. Cybercriminals have come up with a new way of duping unsuspecting bank customers into handing over their funds. They promote shady insurance that supposedly protects against losses caused by online banking fraud. Trusteer experts have detailed the way these attacks work and how they leverage the Tatanga malware platform to ensure the success of the malicious campaign. First, the malware informs the victim of the allegedly free offer via Web browser injection. Then, the potential victim is presented with a fake insurance account whose value is purportedly equal to the amount of money currently present in the bank account. To activate the new account, the user is asked to authorize the transaction by entering the one-time password the bank sends via SMS to his/her mobile device. In reality, the "insurance account" is a normal account that belongs to a money

mule involved in the scheme. When users authorize the activation, they are actually authorizing a fund transfer from the victim to the mule. Experts have found the crooks steal the entire amount of money from the bank account if the balance is between $1,300 and $6,500. However, if the amount is exceeded, they will only take $6,500. "Once they have compromised an endpoint, the ability of Tatanga and the other cybercrime platforms to commit online fraud is limited only by the imagination of criminals," Trusteer's chief technology officer said. Source: http://news.softpedia.com/news/Tatanga-Malware-Platform-Used-in-Fraud-Insurance-Scam-268275.shtml

Iowa man convicted in bomb plot targeting financial firms. An Iowa man was convicted May 4 of mailing pipe bombs and threatening letters to investment companies in a failed bid to get the firms to artificially drive up the value of certain stocks. A jury in Chicago found the man guilty of one count of using a destructive device while mailing a threatening communication, two counts of possessing an unregistered destructive device, and nine counts of mailing a threatening communication. Prosecutors said the man, writing under the name "The Bishop," sent a series of letters to financial institutions in 2005, demanding they move a number of stocks he had an interest in to specific price targets by specific dates. The U.S. Postal Inspection Service, which led the 100-person-member task force that investigated the mailings and ultimately tracked them to the man, said the letters and packages contained recurring phrases, including "Life is full of choices," "Bang you're dead," and "Tic-Toc." Prosecutors said the man's motive was financial. At trial, they presented evidence he had opened option contracts in two of the firms mentioned in the letters, and the value of those positions would have increased if the underlying stocks had moved in the direction he demanded. The mailings took an ominous turn in 2007 when American Century Investment Management in Kansas City, Missouri, and Janus Capital Group in Denver received threatening notes and functional, but disarmed, pipe bombs. The device sent to Denver was rerouted to the firm's Chicago office where police intercepted it. On the day the suspect was arrested, investigators recovered two additional assembled pipe bombs in a storage locker he rented that were similar to the mailed ones. Source: http://www.chicagotribune.com/news/sns-rt-us-crime-bomber-iowabre844005-20120504,0,1448561.story

Chemical and Hazardous Materials Sector

Panel: Chemical industry needs guidance in choosing processing methods to reduce hazards. The chemical industry needs guidance in choosing alternative processing methods to reduce or eliminate hazards, a national panel said in a report released May 11. U.S. Occupational Safety and Health Administration rules require chemical firms to follow certain procedures to ensure manufacturing processes are safe. However, the report by the National Research Council said the industry lacks common practice protocols and understanding to identify safer processes. It recommends the U.S. Chemical Safety Board or another entity develop a plan to help chemical plant managers choose alternative processes to reduce or eliminate hazards. The report said current protocols do not always provide clear guidance, citing the "inherently safer process" method as an example. The report said switching to a non-flammable solvent in a process could remove a fire hazard. But, if the solvent is toxic, a new hazard is created. Congress ordered the

study after a 2008 explosion at BayerCropscience's plant in Kanawha County, West Virginia, killed two workers. The explosion occurred near a storage tank containing methyl isocyanate, a highly toxic chemical known as MIC. The tank was not damaged and the chemical was not released. Bayer took steps to reduce risks associated with MIC manufacturing and storage. However, it did not incorporate all possible methods to control hazards, the report said. Source: http://www.therepublic.com/view/story/6da293e868e2452480b666aa521f16a7/WV--Chemical-Safety/

EPA to remove vapor-capturing rubber boot from gas pump handles. The U.S. Presidential Administration and the Environmental Protection Agency (EPA) announced May 10 they intend to phase out the rubber boots on gas pump handles now used to capture harmful gasoline vapors while refueling cars. The EPA said the vapor-capturing fuel pumps are redundant because more than 70 percent of all cars on the road today are equipped with on-board systems that capture the harmful vapors. According to the EPA, 31,000 affected gas stations in mostly urban areas where smog is a problem will each save $3,000 apiece once the ruling is fully implemented. The most obvious gas vapor recovery system for drivers is the rubber boot at the end of the fuel pump nozzle that fits directly over the gas tank opening. When drivers refuel, gas vapors can escape and contribute to smog and harmful air pollution. To combat the release of these vapors, most gas stations have installed special gas pump nozzles that include the rubber boot to block vapors from escaping. The EPA said the rubber fittings will be phased out as part of the new rule. The Administration said in a statement it hopes the May 10 move will save consumers and businesses almost $6 billion in the next 5 years. Source: http://www.koco.com/news/politics/EPA-to-remove-vapor-capturing-rubber-boot-from-gas-pump-handles/-/9843896/13066998/-/v8mpha/-/

EPA promotes safer alternatives to nonylphenol ethoxylates. May 9, the U.S. Environmental Protection Agency (EPA) released the final report on alternatives to nonylphenol ethoxylates (NPEs) through the Design for the Environment (DfE) Alternatives Assessment Program. NPEs are widely used surfactants with a range of industrial applications and are commonly found in consumer products, such as laundry detergents. When released into the environment, they can be persistent and highly toxic to aquatic organisms. The report identifies eight safer alternatives to NPEs that meet EPA's criteria for safer surfactants. It provides information on the availability of safer alternatives, DfE's hazard evaluation method for surfactants, and the progress being made in adopting safer surfactants. Using rigorous hazard-based criteria, EPA evaluated hundreds of chemicals for their biodegradability and their potential effects to aquatic organisms. Source: http://yosemite.epa.gov/opa/admpress.nsf/0/837566f324a4bbbf852579f90069ba00?OpenDocument

Commercial Facilities

Malware installed on travelers' laptops through software updates on hotel Internet connections. Recent analysis from the FBI and other government agencies demonstrates that malicious actors are targeting travelers abroad through pop-up windows while establishing an

Internet connection in their hotel rooms, the Internet Crime Complaint Center reported May 8. Recently, there have been instances of travelers' laptops being infected with malicious software while using hotel Internet connections. In these instances, the traveler was attempting to setup the hotel room Internet connection and was presented with a pop-up window notifying the user to update a widely-used software product. If the user clicked to accept and install the update, malicious software was installed on the laptop. The pop-up window appeared to be offering a routine update to a legitimate software product for which updates are frequently available. The FBI recommended that all government, private industry, and academic personnel who travel abroad use extra caution before updating software while connected to hotel Internet connections. Source: http://www.ic3.gov/media/2012/120508.aspx

(Massachusetts) **Chemical suicide shuts down Seekonk carnival.** Fire officials in Seekonk, Massachusetts, believed a man killed himself May 5 by breathing in a mixture of hydrogen sulfide while inside a car, in a parking lot, where a carnival was scheduled to take place. The man left several notes on the car warning people to stay away. Without those warnings, officials said the situation could have been much worse. After HAZMAT crews got inside the car, they found the man inside was dead. The man was poisoned by two buckets filled with hydrogen sulfide, which could have been deadly to others if it had escaped the car. Investigators concluded the man used the gas to commit suicide. The carnival was scheduled to begin as planned May 6. Source: http://www.abc6.com/story/18152628/chemical-suicide-shuts-down-seekonk-carnival

Communications Sector

FTC looks to force billing company to pay $52 million for bogus charges. The U.S. Federal Trade Commission (FTC) has asked a federal court to force a third-party billing company to pay $52.6 million for allegedly placing unauthorized charges on consumer phone bills, The Hill reported May 8. The practice of putting unwanted third-party charges on phone bills is known as "cramming," and is the target of potential regulations by the Federal Communications Commission (FCC) and Congress. According to the FTC's court filing, Billing Services Group (BSG) placed charges on nearly 1.2 million telephone lines on behalf of a serial phone crammer. The charges were for "enhanced services," such as voice mail, identity theft protection, directory assistance, job skills training, and video streaming. Consumers never asked for the services. BSG continued billing customers despite "voluminous" complaints and the fact that few customers ever used the services they were charged for, the FTC said. According to the government's motion, BSG billed more than 250,000 consumers for a streaming video service, but only 23 movies were streamed — some of them by the cramming firm's employees. BSG placed $70 million in bogus charges and only refunded about $17.4 million, according to the FTC. The FCC adopted a rule last month to try to combat cramming. The regulation requires landline telephone companies to notify consumers if they have the option to block third-party charges and strengthens rules requiring companies to list the charges separately on bills.Source: http://thehill.com/blogs/hillicon-valley/technology/225999-ftc-looks-to-force-billing-company-to-pay-52-million-for-bogus-charges

Critical Manufacturing

NHTSA recall notice - Ford Expedition, F-150, Mustang, and Lincoln Navigator reverse indicator lights. Ford announced May 10 the recall of 10,500 model year 2011-2012 Ford F-150, 2012 Expedition and Lincoln Navigator, and 2012-2013 Mustang vehicles, for failing to comply with federal motor vehicle safety standards. These vehicles may have a transmission range sensor (TRS) calibrated out of specification for reverse gear. If this condition exists, the transmission may not go into reverse, or when the driver pushes the shift lever in the reverse "R" position and the vehicle's transmission does go in reverse, the "R" may not illuminate on the dashboard of the F-150, Expedition, or Navigator models and/or the backup lamp on the rear of the F-150, Expedition, Navigator, or Mustang vehicles may not illuminate. These conditions increase the risk of a crash or a pedestrian being struck due to the vehicle's not signaling it is in reverse. Ford will notify owners, and dealers will inspect and replace the TRS as necessary. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V190000&summary=true&prod_id=1420768&PrintVersion=YES

Ford adds Virginia to Windstar minivan recall. Ford Motor Co. added 27,000 Windstar minivans from Virginia to a larger recall because the rear axles can crack and fail, the Associated Press reported May 9. The vans are now part of an August 2010 recall of more than 600,000 Windstars in the United States and Canada from the 1998 through 2003 model years. Ford said at the time the vans were sold in states where salt is used to clear the roads. Over time, the salt can cause the axles to rust, crack, and even break, causing a driver to lose control. Virginia was not included in the original recall. However, Ford said a recent analysis showed vans there can have similar problems. There were 11 reports of axle cracks from Virginia between October 2011 and March. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2012/05/09/financial/f061203D68.DTL

NHTSA recall notice - International Lonestar, Paystar, Prostar, Transtar, and Workstar alternator cable fire hazard. Navistar announced May 8 the recall of 19,264 model year 2010-2013 Paystar, Workstar, Transtar, and Prostar, and model year 2012-2013 Lonestar commercial trucks manufactured from June 1, 2009 through April 4, equipped with a Maxxforce 11 or 13 engine and with certain Bosch alternators. The alternator cable may rub on the high pressure power steering hose, possibly chafing its insulation and causing an electrical short. A short may cause a vehicle fire possibly resulting in property damage, personal injury, or death. Navistar will install a standoff bracket and improve harness routing to better route the alternator wires away from the power steering hose. Navistar did not provide an expected start date for the recall, but an interim notice will be mailed to owners if parts will not be available before June 30. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V196000&summary=true&prod_id=1154774&PrintVersion=YES

NHTSA recall notice - Chrysler 300 and Dodge Charger antilock brake control unit. Chrysler announced May 7 it is recalling 119,072 model year 2011 and 2012 Chrysler 300 and Dodge

Charger vehicles. These vehicles may lose antilock braking system/electronic stability control (ABS/ESC) system function due to an overheated power distribution center. This could lead to loss of vehicle control, increasing the risk of a crash. Chrysler will notify owners, and dealers will relocate the ABS/ESC system fuse. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V197000&summary=true&prod_id=1209772&PrintVersion=YES

Defense/ Industry Base Sector

Hypoxia-like illness also hits F-22 maintainers. Oxygen problems plaguing the U.S. Air Force's F-22 stealth fighter are afflicting maintainers working on the plane — as well as pilots — with dizziness, nausea, and other hypoxia-like symptoms, the Air Force Times learned. At least five ground maintainers complained of illness between September and December 2011, an Air Combat Command spokesman said in an Air Force Times article released May 7. The maintainers grew sick after breathing in ambient air during ground engine runs, a Congressional aide told the Air Force Times. The Air Force's investigation into the oxygen problems with the jet, which includes at least 11 cases of unexplained hypoxia-like incidents from pilots in the Raptor since its grounding was lifted in September 2011, has expanded to look at the maintainer incidents, the head of Air Combat Command said April 30. The Air Force is in the process of providing maintainers with off-the-shelf canisters to trap and release air during maintenance if they experience breathing problems. The basketball-sized containers, called Summa canisters, measure air quality around maintainers. They can take an air sample with the turn of a valve if maintainers smell or feel anything unusual. Source: http://www.airforcetimes.com/news/2012/05/air-force-f22-maintainers-illness-050712/

Emergency Services

Police-themed ransomware targets U.S., Canadian users. A ransomware application that locks computers and asks their owners to pay fines for allegedly violating several laws through their online activity is targeting U.S. and Canadian users, malware experts from security firm Trend Micro said May 9. The Trend Micro researchers refer to this particular ransomware — malware that disables system functionality and asks for money to restore it — as the "Police Trojan," because it displays rogue messages claiming to originate from law enforcement agencies. The "Police Trojan" appeared in 2011 and originally targeted users from several countries in Western Europe, including Germany, Spain, France, Austria, Belgium, Italy, and the United Kingdom. The rogue message displayed after locking down a victim's computer is localized in the victim's language and claims to be from a national law enforcement agency from the victim's country. The owners of the locked-down computers are told their IP addresses were involved in illegal activities and are asked to pay a fine using prepaid cards like Ukash or Paysafecard. The malware's authors prefer these payment services because transactions cannot be reversed and are hard to trace. When investigating new command and control servers recently used by this malware, Trend Micro researchers found message templates designed for U.S. and Canadian users. This suggests the malware's scope was extended to these two countries. Source:

http://www.computerworld.com/s/article/9227015/Police_themed_ransomware_targets_U.S._Canadian_users

(Arizona) **Grenades found in Ariz. home where 5 shot dead.** Investigators said they found a half dozen grenades among the military munitions in a suburban Phoenix home where a former Marine with ties to neo-Nazi groups shot four people and then took his own life, the Associated Press reported May 5. An agent from the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) said May 3 the agency is tracing the serial numbers of six 40 mm projectile grenades discovered in the suspect's house. The ATF agent said the explosives were strictly military-issue and should not be in a residence. Officials from Luke Air Force Base took the grenades and destroyed them. The manager of an Army surplus store in Phoenix said that type of grenade is not available at any store. Source: http://www.military.com/news/article/grenades-found-in-ariz-home-where-5-shot-dead.html

(Virginia) **Virginia responder charged in fatal ambulance crash.** EMS World reported May 6 the driver of a Virginia ambulance involved in a wreck that claimed the life of a civilian was charged with reckless driving. The driver did not have the ambulance's lights and siren activated when it collided with a truck in an intersection, according to WSLS 10 Roanoke. Source: http://www.emsworld.com/news/10710231/virgina-responder-charged-in-fatal-ambulance-crash

ENERGY

Feds: Pipeline companies must keep safety records. Energy companies will need to keep up-to-date records to prove they are running the nation's aging pipelines at safe pressures under a new set of guidelines the federal government announced May 7 in response to a deadly natural gas explosion in a San Francisco suburb. If pipeline operators cannot ensure their oil and gas lines are running at safe pressures by 2013, the Pipeline and Hazardous Materials Safety Administration (PHMSA) said they could face penalties or other sanctions. The advisory bulletin the administration issued mentioned the September 2010 gas pipeline explosion in San Bruno that killed 8 people, injured many more and left 38 homes in smoking ruins. Federal and state officials will be responsible for enforcing the new guidelines, a pipeline safety agency spokeswoman said. All companies will be required to keep traceable, verifiable, and complete records about pipelines that ferry hazardous fuels through the nation's most populated areas. In a later phase, the PHMSA also will direct energy firms on what to do if they cannot find records for all their pipelines, she added. Source: http://www.wset.com/story/18168812/feds-pipeline-companies-must-keep-safety-records

Gas pipeline cyber intrustion campaign. In March, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) identified an active series of cyber intrusions targeting natural gas pipeline sector companies, ICS-CERT reported May 4. Various sources provided information to ICS-CERT describing targeted attempts and intrusions into multiple natural gas pipeline sector organizations. Analysis of the malware and artifacts associated with these cyber attacks has positively identified this activity as related to a single campaign. It appears to have

started in December 2011 and remains active. Analysis showed the spear-phishing attempts have targeted a variety of personnel within these organizations; however, the number of persons targeted appears to be tightly focused. In addition, the e-mails have been convincingly crafted to appear as though they were sent from a trusted member internal to the organization. ICS-CERT has issued an alert to the United States Computer Emergency Readiness Team Control Systems Center secure portal library and also disseminated them to sector organizations and agencies to ensure broad distribution to asset owners and operators. ICS-CERT is currently engaged with multiple organizations to identify the scope of infection and provide recommendations for mitigating it and eradicating it from networks. Source: http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf

(Pennsylvania) **Man charged in theft of copper from power company's substations.** A suspect was apprehended May 4 at a Met-Ed substation in Amity Township, Pennsylvania, police said. The man confessed to police his role in 19 recent thefts at substations around Berks County. More than 1,200 pounds of copper tubing was taken in the recent thefts, costing Met-Ed more than $100,000 in materials and repairs. Investigators said the suspect hit substations, and then would break in again to steal more copper after repairs were made. Detectives said the suspect would cash in the copper at a scrap dealer, but due to a Pennsylvania law requiring scrap dealers to keep customer information, police were able to track the transactions. Authorities said the man netted $4,000 in his sale of copper and copper-plated tubing. He faces charges of burglary, theft, and receiving stolen property. Source: http://www.wfmz.com/news/news-regional-berks/Man-charged-in-theft-of-copper-from-power-company-s-substations/-/121418/12563850/-/yp3vrmz/-/index.html

Food and Agriculture

More frozen tuna from India recalled due to Salmonella risk. The company in India that supplied the yellowfin tuna implicated in the multistate outbreak of Salmonella infections linked to sushi recalled 22-pound cases of frozen tuna strips because they may also be contaminated with Salmonella. In a news release May 9, Moon Fishery said the U.S. Food and Drug Administration (FDA) isolated Salmonella in a sample of tuna strips that had not yet been distributed. As a cautionary measure, it agreed to recall frozen tuna strips that had already been shipped, although it said none of those shipments "is from the suspect lot sampled by the FDA." The recalled tuna strips were shipped to four wholesalers in Georgia, Massachusetts, New Jersey, and New York. Moon India said distribution of its tuna was suspended while the FDA continued its investigation. As of May 2, 258 people infected with Salmonella Bareilly or Salmonella Nichanga were reported from 24 states and Washington, D.C., according to the Centers for Disease Control and Prevention (CDC). The CDC said frozen yellowfin tuna, called Nakaochi Scrape, imported from India was the likely source. Many of those sickened reported eating sushi — in particular "spicy tuna sushi" — in the week before they became ill. Moon Marine USA Corp. of Cupertino, California, recalled 58,828 pounds of Nakaochi Scrape.Source: http://www.foodsafetynews.com/2012/05/tuna-strips-from-india-recalled-due-to-salmonella-risk/

Solid Gold Health Products for Pets, Inc. recalls dog food because of possible Salmonella health risk. Solid Gold Health Products for Pets, Inc. of El Cajon, California, announced a voluntary recall of one batch of WolfCub Large Breed Puppy Food and one batch of Solid Gold WolfKing Large Breed Adult Dog, the U.S. Food and Drug Administration reported May 8. Solid Gold voluntarily recalled the products that were distributed in the United States and Canada. This voluntary recall was being done as these products were produced at the facility that was linked to recent recalls of Diamond brand pet foods due to potential Salmonella contamination. Source: http://www.fda.gov/Safety/Recalls/ucm303371.htm

Ontario crops have suffered millions in damage, say growers. The early warm weather in March, followed by sudden flash freezes, caused losses to tender fruit and apple growers in a large part of southern Ontario, Canada, the Canadian Press reported May 9. An agriculture specialist at the University of Guelph said the apple industry alone in Ontario is worth up to $400 million. An official with the Ontario Tender Fruit Producers Marketing Board in Niagara said about 30 percent of peaches and nectarines were affected, with damage totaling about $24 million to those 2 crops alone. Growers will not know the impact on the grape crop until early June. Source: http://www.thestar.com/news/canada/article/1175392--ontario-crops-have-suffered-millions-in-damage-say-growers

Natural Balance Pet Foods initiates voluntary recall of certain dry pet food due to potential for Salmonella contamination. Natural Balance Pet Foods announced May 4 it was issuing a voluntary recall of certain dry pet food formulas manufactured by Diamond Pet Foods at their Gaston, South Carolina facility. Although there have been no animal illnesses reported and none of the products in the recall has tested positive for Salmonella, the company voluntarily initiated this recall as a precautionary measure. Recalled products may have been distributed in Alabama, Arkansas, Colorado, Connecticut, Washington, D.C., Delaware, Florida, Georgia, Iowa, Illinois, Indiana, Kansas, Kentucky, Louisiana, Massachusetts, Maryland, Maine, Michigan, Minnesota, Missouri, Mississippi, North Carolina, North Dakota, Nebraska, New Hampshire, New Jersey, New York, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Virginia, Vermont, Wisconsin, West Virginia, Wyoming, and Canada. Source: http://www.fda.gov/Safety/Recalls/ucm303042.htm

State and federal programs helped catch contaminated dog food. The U.S. Centers for Disease Control and Prevention (CDC) was able to connect contaminated dog food to a Salmonella outbreak spread across nine states May 3 due to a combination of routine State-level testing and a national online infection database operated by the CDC. Several brands of Diamond Pet Foods dry dog food manufactured at a single South Carolina facility tested positive for Salmonella Infantis, a rare strain that infected at least 14 people and hospitalized at least 5. The individuals contracted the illnesses either through handling the tainted kibble or having contact with a dog that had eaten it. The connection between the dog food and the human Salmonella Infantis illnesses first arose after the rare Salmonella strain was discovered in an unopened bag of Diamond Pet Foods kibble during routine retail sampling by the Michigan Department of Agriculture & Rural Development April 2. Knowing the genetic fingerprint of the Salmonella, the CDC consulted PulseNet, its online network that connects public health and regulatory

personnel around the country to share data on disease infections. They found that a handful of human Salmonella infections around the country matched up with the bacteria in the dog food. When public health officials followed up with those individuals, most of them reported an association with Diamond Pets dog food. Source: http://www.foodsafetynews.com/2012/05/state-and-federal-programs-helped-catch-contaminated-dog-food/

(Ohio) **Late frost wreaks havoc on Ohio's grapes, causing concern for growers, winery owners.** Grape growers and winery owners in northern Ohio and nearby states sensed their crops could be damaged when temperatures remained unseasonably high in March, the Cleveland Plain Dealer reported May 5. However, they did not foresee the destruction that occurred April 29. Temperatures in the low to mid-20s caused most grapes to freeze, which could have a dramatic impact on harvest the fall of 2012 for dozens of the state's 163 wineries. Ohio wineries experienced 11 frosts since the middle of March, said the executive director of the Ohio Wine Producers Association in Geneva. Some of the frosts were brief and caused little damage. Part of the problem April 29 was it was too cold for wind machines, which many wineries and grape growers own, to prevent the frost from taking hold. Although the impact of the freeze will not be fully known for several weeks, the executive director said the market will be affected starting in 2013 and possibly extending until 2015. Source: http://www.cleveland.com/taste/index.ssf/2012/05/frost_wreaks_havoc_on_grapes_f.html

Government Sector (including Schools and Universities)

(Ohio) **Four arrested after bomb and shooting threat at Central Catholic High posted on Facebook.** Police in Stark County, Ohio, arrested four teenagers in connection with a bomb and shooting threat at Central Catholic High School in Canton that was posted on Facebook. The Perry Township Police Department said it first got word of the threat May 9 and officers worked throughout the night to investigate the case. School officials decided to cancel school May 10, and police sent in the Summit County Bomb Squad to sweep the school for any explosives. No explosives were found. Four suspects were charged with breaking and entering and inducing panic. Massillon police said those arrested were not students at the school. The four suspects entered the school and posted the threat message on a Facebook page that was left open by a staff member in a classroom. Source: http://www.newsnet5.com/dpp/news/local_news/oh_stark/four-arrested-after-bomb-and-shooting-threat-at-central-catholic-high-posted-on-facebook

(Connecticut) **Powder scares prompt closure of 3 Conn. buildings.** A government building in Waterbury and two schools in Newington and Manchester, Connecticut, remained closed as authorities investigated suspicious white powders discovered by workers May 10. The Rowland State Government Center in Waterbury and Ruth Chaffee Elementary School in Newington were evacuated, and the Keeney Street Elementary School in Manchester was locked down after workers found white powders. All three buildings were closed May 11. Authorities said

the powder at the Manchester school was found in an envelope with a letter that referred to al-Qa'ida. Officials said the powders were being tested. Source: http://www.boston.com/news/local/connecticut/articles/2012/05/11/powder_scares_prompt_closure_of_3_conn_buildings/

(Texas) **FBI takes lead in white powder investigation after 9th found.** May 9, the FBI took lead of the investigation into 9 white powder scares in 2 days in north Texas cities. The latest suspicious package was found at the Mi Escuelita Preschool in Dallas. This marks the seventh Headstart school in 2 days targeted with envelopes containing a "white powdery" substance. An employee of the Mi Escuelita Headstart school opened the mail May 9 when she noticed a white substance spill out of one of the envelopes. Employees said the envelope did not have a return address. Dallas police secured the scene while Plano's HAZMAT team was called in to handle the envelope. Officials evacuated the building where the envelope was opened, including a classroom with 18 children. Schools in Mesquite, Garland, and Irving received similar suspicious mailings. Two other locations, including a church, also received envelopes. All of them were determined to be non-hazardous. Source: http://dfw.cbslocal.com/2012/05/09/fbi-takes-lead-in-white-powder-investigation-after-9th-found/

(Florida) **Florida nabs white supremacists planning 'race war'.** Ten alleged members of a white supremacist group training near Orlando for a "race war" were rounded up in a series of arrests in central Florida, authorities said May 8. The arrests were based on evidence from a confidential informant who infiltrated the neo-Nazi organization known as the American Front (AF) 17 months ago, according to an arrest affidavit. It said the group's alleged local ringleader operated a heavily fortified paramilitary training center for the AF on his isolated property in St. Cloud, Florida. It said he recently plotted a disturbance at Orlando City Hall and a confrontation against a rival skinhead group in coastal Melbourne in a bid to garner media attention, but was also experimenting with the potential manufacture of the biological toxin ricin. The investigation into the AF was conducted by the FBI's Joint Terrorism Task Force and local law enforcement agencies. Source: http://www.reuters.com/article/2012/05/09/us-usa-florida-skinheads-idUSBRE84804Q20120509

(Texas) **Students arrested after bomb threat, hit list found.** Two New Waverly, Texas High School students were arrested the week of April 30 after investigators said one of them created a hit list that included school staff and the U.S. President, and the other called in a bomb threat. The school district superintendent said they first noticed threatening graffiti inside a boy's school bathroom May 2. Administrators launched an investigation that led them to a student who was found in possession of a list of names in his backpack. Deputies alerted the Secret Service who interviewed the student. Walker County deputies searched the student's bedroom, found prohibited weapons, and placed him under arrest. Walker County sheriff's deputies said an anonymous caller phoned the school's front office May 3. When a secretary answered, the caller threatened to blow up a bomb at the school, deputies said. A bomb squad was brought to the campus and hundreds inside the building were evacuated. Several students told the principal they saw a fellow student make the threatening phone call while on campus. The

juvenile was taken into custody. Source: http://www.click2houston.com/news/Students-arrested-after-bomb-threat-hit-list-found/-/1735978/12537726/-/spjym2/-/

NASA, ESA confirm hacks; The Unknowns says systems patched. NASA and the European Space Agency (ESA) confirmed they were recently hacked, ZDNet reported May 4. The hacking group The Unknowns said most of the 10 companies it attacked patched their systems, which was supposedly their goal. "NASA security officials detected an intrusion into the site on April 20 and took it offline," a NASA spokesperson said in a statement. "The agency takes the issue of IT security very seriously and at no point was sensitive or controlled information compromised. NASA has made significant progress to better protect the agency's IT systems and is in the process of mitigating any remaining vulnerabilities that could allow intrusions in the future," it said. "The group used SQL injection ... The use of SQL injection is an admitted vulnerability," an ESA security office manager told ZDNet. "This needs to be addressed at a coding level." Source: http://www.zdnet.com/blog/security/nasa-esa-confirm-hacks-the-unknowns-says-systems-patched/11902

Virginia man accused of threatening to kill U.S. President. A Virginia man was charged with threatening to kill the U.S. President, the Associated Press reported May 6. A criminal complaint filed in federal court in Harrisonburg, Virginia, said the suspect made death threats against the President and threatened to bomb the White House, hotels, and other places, including Philadelphia City Hall, and the site of the former World Trade Center in New York City. An affidavit said the threats were e-mailed to various media outlets. Media outlets report an e-mail sent April 19 to a Roanoke radio station threatened the President's life. The FBI traced the e-mail to the suspect's account. The suspect was ordered to undergo a psychological evaluation. Source: http://www.foxnews.com/politics/2012/05/06/virginia-man-accused-threatening-to-kill-obama/

(Massachusetts) **Powder prompts evacuation at school.** Local and federal law enforcement officials were investigating the origin of a mysterious powder that triggered a full-scale hazardous materials response after it was found May 6 in a boys' bathroom in the basement of Nashoba Regional High School in Bolton, Massachusetts. A custodian discovered the powder, said a State fire official, and a HAZMAT team determined the substance was benign. Personnel from the nearby towns of Lancaster, Clinton, Littleton, and Bolton set up a decontamination tent. In all, 20 people were decontaminated as a precaution. Officials said the substance would be handed over to the FBI's Worcester office, which will perform further testing, in addition to investigating how the substance came to be left in the school. Source: http://bostonglobe.com/metro/2012/05/06/heavy-police-and-fire-response-potentially-hazardous-situation-nashoba-regional-high-school/7dlV14ZiGNqPKXNuUaJ55L/story.html

Information Technology and Telecommunications

APT attackers are increasingly using booby-trapped RTF documents. Booby-trapped Rich Text Format (RTF) documents are one of the most common types of malicious Microsoft Office files that are used to infect computers with advanced persistent threats, according to security

researchers from Trend Micro. The company's statistics show that 63 percent of the malicious Microsoft Office documents intercepted in April exploited vulnerabilities in Microsoft Word. Out of those vulnerabilities, the most commonly targeted ones were CVE-2010-3333 and CVE-2012-0158, which stem from bugs in Microsoft Word's code for parsing RTF content. This is troublesome because Microsoft just patched a new Microsoft Word RTF parsing vulnerability May 8 that could allow remote code execution. Source: http://www.infoworld.com/d/security/apt-attackers-are-increasingly-using-booby-trapped-rtf-documents-192891

Cybersecurity model may benefit a new cloud-based network. In the online struggle for network security, Kansas State University cybersecurity experts are adding an ally to the security force: the computer network itself. Two professors of computing and information sciences are researching the feasibility of building a network that could protect itself against online attackers by automatically changing its setup and configuration. The two researchers were recently awarded a 5-year grant of more than $1 million from the Air Force Office of Scientific Research to fund the study "Understanding and quantifying the impact of moving target defenses on computer networks." The study, which began in April, will be the first to document whether this type of adaptive cybersecurity, called moving-target defense, can be effective. If it can work, researchers will determine if the benefits of creating a moving-target defense system outweigh the overhead and resources needed to build it. Source: http://www.net-security.org/secworld.php?id=12911&utm

Security of industrial control systems questioned at DHS conference. Operators of America's power, water, and manufacturing facilities use industrial control systems (ICS) to manage them. However, the security of these systems, increasingly linked with Microsoft Windows and the Internet, is now under intense scrutiny because of growing awareness that they could be attacked and cause massive disruptions. Industrial facility operators are making efforts to follow security procedures, such as using vulnerability-assessment scanning tools to check for needed patches in Windows. However, ICS environments present special problems, said managers who spoke on the topic at a conference organized by the DHS. Currently, energy and manufacturing facilities are being openly warned by DHS and its Industrial Control Systems Computer Emergency Response Team that they are being targeted by attackers who will often try to infiltrate business networks, often through spear phishing attacks against employees, in order to also gain information about ICS operations. Source: http://news.idg.no/cw/art.cfm?id=F6A00A23-93CE-4ADC-E9CC5545017384EC

Thousands of Twitter passwords allegedly exposed. About 55,000 Twitter account names and passwords, it was claimed May 8, were published on Pastebin May 7. Twitter confirmed it was investigating the situation and said it was resetting the passwords of affected accounts. Later examination of the list by Twitter revealed it contained 20,000 duplicates, suspended spam accounts, and incorrect log-in credentials. It is unclear where the data came from — Mashable said hackers affiliated with Anonymous were involved, but no apparent announcement from the hackers was made. It does not appear Twitter's systems were compromised. A random sampling of a number of the accounts by a Hacker News reader found them to typically have

several followers and to be following thousands of other Twitter users — a common footprint of a Twitter spam account. An analysis by an Eset blogger found that even after deduplicating the list, 25,000 entries in the remaining list were e-mail addresses. This leaves around 9,000 apparent Twitter spam accounts. Eset compared the accounts with previous leaks and found the e-mail ones apparently matched a June 2011 LulzSec leak and also found some of the spam accounts posted in an April 2012 forum post. Source: http://www.h-online.com/security/news/item/Thousands-of-Twitter-passwords-allegedly-exposed-1571195.html

Phishing impersonating email service providers spikes. Phishing attacks impersonating e-mail service providers increased 333 percent from Q4 2011 to Q1 2012. IT security firm Internet Identity (IID) attributes this spike to spammers needing unsullied e-mail addresses since many major spamming botnets have been shut down, and Internet service providers have become more successful at identifying and blocking e-mail from botnets and other known spam sources. During the first quarter of 2012, spammers increasingly tried to hijack "good" e-mail addresses at large Web mail services by impersonating those e-mail service providers and phishing for e-mail account log-in credentials. Despite the dramatic jump in e-mail service provider phishing, other industries on average witnessed a decrease in phishing attacks. IID found phishing attacks dropped 2 percent when comparing statistics from Q1 2011 to Q1 2012. Source: http://www.net-security.org/secworld.php?id=12896&utm

Zombie PCs exploit hookup site in 4Square-for-malware scam. Security researchers discovered a strain of malware that uses the geolocation service offered by an adult dating Web site as a way to determine the location of infected machines. Thousands of infected machines in a zombie network contacted the URL at the adult hookup site, security researchers at Websense discovered. Analysts first thought the adult dating site was abused as a botnet command and control channel. A more detailed look at the traffic from an infected machine revealed JavaScript code built into the malware queried the site's systems to discover the exact location — state, city, latitude, and longitude — of infected PCs. All indications are the site is unaware of this behavior. Instead, its unsecured geo-location services are being used as a kind of 4Square for zombie PCs. This information is "used by the botmaster for statistics or to give different commands to infected machines in certain countries," Websense explains. The security firm reports that in more than 4,700 samples of these yet unnamed malware behind the attack were submitted to its security lab to date. Source: http://www.theregister.co.uk/2012/05/08/geo_location_malware/

1,000+ WordPress sites compromised through automatic update feature. More than 1,000 WordPress blogs were modified to redirect visitors to sites serving malware, affiliate, and pay-per-click redirectors and low quality PPC search result aggregators through the WordPress' automatic update feature. The individuals behind the attack discovered how to add the malicious code to the update.php file, which prompts WordPress to update. This code then injects other code in the wp-settings.PHP file, and effects the redirects. Source: http://www.net-security.org/secworld.php?id=12865

Phishers mimic OpenID to steal credentials. New spam e-mail campaigns are taking advantage of the users' vague familiarity with the OpenID authentication method to phish their log-in credentials for many different and popular online services, warn Barracuda Labs researchers. The e-mails in question currently take the form of an offer from a real estate company or of a bogus UPS tracking alert. After following the offered link, users are presented with a fake log-in page hosted on a compromised site. The page itself does not mention OpenID, but the logos of large and popular Web sites that use and provide the option of OpenID authentication (Google, AOL, Yahoo!, etc.) can fool users into thinking the page is legitimate. Whichever e-mail the user selects, a pop-up window requesting log-in credentials appears. "This is not how OpenID authentication works," the researchers point out. With genuine OpenID authentication we would be directed to a secure Yahoo Web page which would ask for credentials." In this case, the inputed credentials are simply forwarded in plain text to a remote server operated by the phishers, and the user is redirected to the real estate agency's or UPS' legitimate Web site. Source: http://www.net-security.org/secworld.php?id=12874&utm

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

(Georgia) **Police: Trio targeted Treasury Department checks in mail thefts.** Atlanta police said they arrested three people targeting people's checks by stealing their mail, WSB 2 Atlanta reported May 8. A postal inspector told an Atlanta police officer at the scene of a May 1 theft at the Heritage Green Apartments that the trio may be the ones who have been breaking into cluster mailboxes. The inspector said the U.S. Department of the Treasury mails out checks at the first of the month. Atlanta police investigated two other mail thefts where mail carriers said the trio also swiped mail from their trucks. Police said they spotted the suspects' car at a check cashing business, where they arrested all three and found a stack of checks in the car. They are now facing felony theft charges. A postal inspector noted stealing mail is a federal offense. The Postal Service sent a letter to people in the area that said to contact them if their Treasury check was cashed by someone else. Source: http://www.wsbtv.com/news/news/local/police-trio-targeted-treasury-department-checks-ma/nNyjZ/

Public Health

(Kansas) **Johnson County sees outbreak of whooping cough.** Health officials in Johnson County, Kansas, said May 9 the county has seen an outbreak of whooping cough in 2012. The county said 70 confirmed or probable cases of whooping cough were reported in the county in 2012. The Johnson County Department of Health and Environment said people who have regular contact with infants should get a Tdap vaccine. Health care providers were being urged to consider the possibility of whooping cough when evaluating patients with a serious cough. Source: http://www.ksn.com/news/state/story/Johnson-County-sees-outbreak-of-whooping-cough/NuVxBncp5kOhu1Thefo50Q.cspx

(Colorado) **Whooping cough outbreak: Seven confirmed cases at University middle school.** The number of confirmed cases of whooping cough at University middle school in Greeley, Colorado, climbed to seven, including one teacher, leading school officials to ban all students who are not immunized from the building, the Greeley Tribune reported May 9. The school nurse said the number of confirmed cases continues to rise, and health department officials made several recommendations to the school to get the outbreak of the pertussis infection under control. "The school sent home three letters Wednesday to different groups of students based on Weld County Department of Public Health and Environment's findings," said University Schools' director. One letter went to the parents of middle school athletes on the track team, which is where the health department believes the cases originated. Source: http://www.greeleytribune.com/article/20120509/NEWS/705099959/1007&parentprofile=1025

Report: Suspect billings at 2,600 drugstores. May 10, the Associated Press reported that Medicare paid $5.6 billion to 2,600 pharmacies with questionable billings, including a Kansas drugstore that submitted more than 1,000 prescriptions each for 2 patients in just 1 year, government investigators found. A new report by the inspector general of the Health and Human Services department found the corner drugstore vulnerable to fraud, partly because Medicare does not require the private insurers that deliver prescription benefits to seniors to report suspicious billing patterns. The analysis broke new ground by scrutinizing every claim submitted by the nation's 59,000 retail pharmacies during 2009 — more than 1 billion prescriptions. Investigators were able to reveal contrasts between normal business practices and potential criminal behavior. "The findings call for a strong response to improve (program) oversight," the report said. In written comments, a Medicare administrator said the agency mostly agrees with the inspector general's call to action. Source: http://www.ktvn.com/story/18249095/apnewsbreak-suspect-billings-at-2600-drugstores

(Washington) **Whooping cough forces emergency closure of Blanchet.** After more than 150 students called in sick May 8, Bishop Blanchet High School in Seattle declared an emergency closure for at least May 9 and May 10 due to whooping cough. According to a May 8 letter sent to parents, the principal consulted with the Seattle/King County Health Department and the Catholic Schools Department before making the decision to close. The principal asked parents to report sick children even during the closure so the school can track the illness. Washington State is currently experiencing a whooping cough epidemic, with more than 1,100 cases reported in 2012. Source: http://www.seattlepi.com/local/komo/article/Whooping-cough-forces-emergency-closure-of-3543712.php

U.S. Senate panel launches investigation of painkillers, drug companies. The Milwaukee Journal Sentinel reported May 9 the U.S. Senate Committee on Finance opened a bipartisan investigation into financial relationships between companies that make narcotic painkillers and various non-profit organizations that have advocated their use for the treatment of pain. Citing investigative reports by the Milwaukee Journal Sentinel, MedPage Today, and others, the committee is seeking financial and marketing records from three companies that make opioid

drugs, including Oxycontin and Vicodin, and seven national organizations. "It is clear that the United States is suffering from an epidemic of accidental deaths and addiction resulting from increased use of powerful narcotic painkillers," said a joint statement from committee members. The Senators said there was growing evidence that drug companies have promoted misleading information about the safety and effectiveness of the drugs with help from nonprofits they have donated to. Source: http://www.jsonline.com/watchdog/watchdogreports/us-senate-panel-launches-investigation-of-painkillers-drug-companies-4u5arr1-150767225.html

Abbott Laboratories to pay $1.6 billion over misbranding drug. Abbott Laboratories pleaded guilty and agreed to pay $1.6 billion to resolve its criminal and civil liability arising from the company's unlawful promotion of the prescription drug Depakote, the U.S. Department of Justice (DOJ) said May 7. The total includes a criminal fine of $700 million and civil settlements with states and the federal government totaling $800 million. Separate from the DOJ settlement, Abbott agreed to pay 45 states a total of $100 million to resolve liability under the state consumer-protection laws. That makes this the second-largest fraud settlement involving a drug company, behind only a $2.3 billion Pfizer settlement in 2010. Abbott pleaded guilty to misbranding Depakote by promoting the drug to control agitation and aggression in patients with elderly dementia, and to treat schizophrenia when neither use was approved by the U.S. Food and Drug Administration. Source: http://www.cnn.com/2012/05/07/justice/abbott-fine-drug/index.html?hpt=hp_t3

TRANSPORTATION

U.S. scales back railroad safety rules. The White House announced May 10 that it will scale back federal rail safety rules spurred by a 2008 train collision in the Chatsworth section of Los Angeles that killed 25 people and hurt 135 others. The administration said it will slash by 10,000 miles the amount of railroad track that must be covered by systems that can override human error and automatically put the brakes on trains about to collide or derail. Known as Positive Train Control (PTC), the high-tech systems previously were projected to cover an estimated 70,000 miles of track used by trains carrying passengers or extremely hazardous materials such as chlorine. The safeguards were due to be installed by the end of 2015 under legislation passed by Congress in response to the deadly head-on, Chatsworth train crash. Over 20 years, the Transportation Department said, the regulatory change will save railroads up to $775 million, reducing the overall cost of installing and operating PTC over that period to about $12.3 billion. Metrolink, operator of the commuter train that was involved in the head-on collision with a freight train in the deadly 2008 California accident, has become a leading advocate of PTC. Source: http://www.contracostatimes.com/california/ci_20598367/u-s-scales-back-railroad-safety-rules

Safety Board highlights dangers of hose-chemical incompatibility. The National Transportation Safety Board (NTSB) asked the Department of Transportation to warn trucking companies about the dangers of not using the right hoses for the right chemicals, after determining the use of a cargo hose assembly that was not chemically compatible with anhydrous ammonia caused a

fatal 2009 accident, Trucking Info reported May 10. A cargo transfer hose ruptured July 15, 2009, shortly after transfer of anhydrous ammonia began from a Werner Transportation cargo tank truck to a storage tank at the Tanner Industries facility in Swansea, South Carolina. NTSB investigators determined the probable cause of the accident was Werner's use of a cargo hose assembly designed for liquefied petroleum gas (LPG) transfer only and was not chemically compatible with anhydrous ammonia. As a result of the investigation, the NTSB issued a joint recommendation to the DOT's Federal Motor Carrier Safety Administration and Pipeline and Hazardous Materials Safety Administration to "jointly issue a safety advisory bulletin to inform cargo tank motor vehicle owners and operators, registered inspectors of these vehicles, and transfer facility operators about the circumstances of this accident and actions needed to prevent the occurrence of a similar accident." Source: http://www.truckinginfo.com/news/news-detail.asp?news_id=76892

CIA thwarts Al Qaeda underwear bomb plot near anniversary of leader's death. A team of FBI experts were examining a sophisticated, new al-Qa'ida bomb to figure out whether it could have slipped past airport security and taken down a commercial airplane, U.S. officials said. The bomb was confiscated after the CIA unraveled a terror plot by al-Qa'ida in the Arabian Peninsula to destroy a U.S.-bound airliner using an underwear bomb, Fox News reported May 8. The plot involved an upgrade of the underwear bomb that failed to detonate aboard a jetliner over Detroit December 25, 2009. This new bomb was also designed to be used in a passenger's underwear, but this time al-Qa'ida developed a more refined detonation system, U.S. officials told the Associated Press. "Initial exploitation indicates that the device is very similar to IEDs that have been used previously by Al Qaeda in the Arabian Peninsula in attempted terrorist attacks, including against aircraft and for targeted assassinations," the FBI said in a written statement. "The FBI currently has possession of the IED and is conducting technical and forensics analysis on it." Officials said the device did not contain metal, meaning it probably could have passed through an airport metal detector. However, it was not clear whether new body scanners used in many airports would have detected it. It was not clear who built the bomb, but because of its sophistication and its similarity to the Christmas bomb, authorities suspected it was the work of a master bomb maker who constructed the first underwear bomb and two others al-Qa'ida built into printer cartridges and shipped to the U.S. on cargo planes in 2010. Source: http://www.foxnews.com/us/2012/05/07/cia-thwarts-al-qaeda-underwear-bomb-plot-on-anniversary-bin-laden-death-us/?test=latestnews

Water and Dams

(Idaho) **Star mayor declares state of emergency due to flooding.** The mayor of Star, Idaho, declared a state of emergency May 8 in response to two levee breaches along the Boise River. The water flooded over some canals into some nearby fields and ditches in the area. The declaration allows the city to be eligible for more funding and aid, but the mayor said flood crews in Ada County repaired the breaches without additional help. Some flooding remained in the fields and ditches but no buildings were damaged as of May 9. The Boise River was flowing at 8,000 cubic feet per second (cfs) and expected to remain at that level as the U.S. Army Corps of Engineers continues to release water from the upstream reservoirs. Flood stage is considered

7,000 cfs. Source: http://www.kboi2.com/news/local/Star-mayor-declares-state-of-emergency-due-to-flooding-150711245.html

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168